ATTACHMENTS

REQUEST FOR APPLICATIONS

Debt Free DC in 2023 Grant:

Helping DC Residents Eliminate Outstanding Medical Debt

A) **Application**
B) **Statement of Certifications**
(and B2 if a subgrantee is being utilized)
C) **DHCF RFA Receipt**
D) **HIPAA Checklist**

GOVERNMENT OF THE DISTRICT OF COLUMBIA

DEPARTMENT OF HEALTH CARE FINANCE (DHCF)

Statement of Certification

A. Applicant/Grantee has provided the individuals, by name, title, address, and phone number who are authorized to negotiate with the Agency on behalf of the organization; (attach)

B. Applicant/Grantee is able to maintain adequate files and records and can and will meet all reporting requirements;

C. All fiscal records are kept in accordance with Generally Accepted Accounting Principles (GAAP) and account for all funds, tangible assets, revenue, and expenditures whatsoever; that all fiscal records are accurate, complete and current at all times; and that these records will be made available for audit and inspection as required by the Grant Administrator;

D. All costs incurred under this grant must be in accordance with the Office of Management and Budget (OMB) Circular A-122, "Cost Principals for Non-Profit Organizations."

E. Applicant/Grantee states whether it, or where applicable, any of its officers, partners, principles, members, associates or key employees, within the last three (3) years prior to the date of the application, has:
   a. Been indicted or had charges brought against them (if still pending) and/or been convicted of:
      i. Any crime or offense arising directly or indirectly from the conduct of the applicant's organization, or
      ii. Any crime or offense involving financial misconduct or fraud; or
   b. Been the subject of legal proceedings arising directly from the provision of services by the organization.

F. If any response to the disclosures referenced in (E.) is in the affirmative, the applicant shall fully describe such indictments, charges, convictions, or legal proceedings (and the status and disposition thereof) and surrounding circumstances in writing and provide documentation of the circumstances.

G. Applicant/Grantee is in compliance with D.C. Official Code § 1-328.15.

H. Applicant/Grantee is current on payment of all federal and District taxes, including Unemployment Insurance taxes and Workers' Compensation premiums. This statement of certification shall be accompanied by a certificate from the District of Columbia OTR stating

that the entity has complied with the filing requirements of District of Columbia tax laws and has paid taxes due to the District of Columbia, or is in compliance with any payment agreement with OTR; (attach)

I. Applicant/Grantee has the demonstrated administrative and financial capability to provide and manage the proposed services and ensure an adequate administrative, performance and audit trail;

J. That, if required by the grant making Agency, the Applicant/Grantee is able to secure a bond, in an amount not less than the total amount of the funds awarded, against losses of money and other property caused by fraudulent or dishonest act committed by any employee, board member, officer, partner, shareholder, or trainee;

K. That the Applicant/Grantee is not proposed for debarment or presently debarred, suspended, or declared ineligible, as required by Executive Order 12549, "Debarment and Suspension," and implemented by 2 CFR 180, for prospective participants in primary covered transactions and is not proposed for debarment or presently debarred as a result of any actions by the District of Columbia Contract Appeals Board, the Office of Contracting and Procurement, or any other District contract regulating Agency;

L. That the Applicant/Grantee has the financial resources and technical expertise necessary for the production, construction, equipment and facilities adequate to perform the grant or sub-grant, or the ability to obtain them;

M. That the Applicant/Grantee has the ability to comply with the required or proposed delivery or performance schedule, taking into consideration all existing and reasonably expected commercial and governmental business commitments;

N. That the Applicant/Grantee has a satisfactory record of performing similar activities as detailed in the award or, if the grant award is intended to encourage the development and support of organizations without significant previous experience, that the Applicant/Grantee has otherwise established that it has the skills and resources necessary to perform the grant. In this connection, Agencies may report their experience with an Applicant/Grantee's performance to OPGS which shall collect such reports and make the same available on its intranet website.

O. That the Applicant/Grantee has a satisfactory record of integrity and business ethics;

P. That the Applicant/Grantee has the necessary organization, experience, accounting and operational controls, and technical skills to implement the grant, or the ability to obtain them;

Q. That the Applicant/Grantee is in compliance with the applicable District licensing and tax laws and regulations;

R. That the Applicant/Grantee complies with provisions of the Drug-Free Workplace Act; and

S. That the Applicant/Grantee meets all other qualifications and eligibility criteria necessary to receive an award under applicable laws and regulations.

T. That the Applicant/Grantee agrees to indemnify, defend and hold harmless the Government of the District of Columbia and its authorized officers, employees, agents and volunteers

from any and all claims, actions, losses, damages, and/or liability arising out of this grant or sub-grant from any cause whatsoever, including the acts, errors or omissions of any person and for any costs or expenses incurred by the District on account of any claim therefore, except where such indemnification is prohibited by law.

As the duly authorized representative of the Applicant/Grantee, I hereby certify that the Applicant/Grantee will comply with the above certifications.

Applicant/Grantee Name: _____

_____ **City** _____ **State** _____ **Zip Code** _____
Street Address

RFA Number: _____ **Applicant IRS Number:** _____

Signature: _____ **Date:** _____

Name and Title of Authorized Representative: _____

_____

C) DHCF RFA Receipt

GOVERNMENT OF THE DISTRICT OF COLUMBIA

DEPARTMENT OF HEALTH CARE FINANCE (DHCF)

Application Receipt

RFA: Debt Free DC in 2023 Grant:

Helping DC Residents Eliminate Outstanding Medical Debt

The DC Department of Health Care Finance is in receipt of:

_____

(Contact Name)

_____

(Organization Name)

_____

_ (Contact Telephone and Email)

[DHCF USE ONLY]

Date Received: ____/____/____ Time Received: ____/____/____

# of Copies received: _____

Received by: _____

D) HIPAA Checklist

HIPAA Security Checklist

HIPAA SECURITY RULE REFERENCE	SAFEGUARD *(R) = Required; (A) = Addressable*	STATUS *(Complete, N/A, etc.)*
	Administrative Safeguards	
164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	
164.308(a)(1)(ii)(A)	Has a Risk Analysis been completed IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the Risk Management process been completed IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)	
164.308(a)(2)	Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	
164.308(a)(3)(i)	Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine that the Access of an employee to EPHI is appropriate? (A)	

Last Updated – 9/6/16

164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves you organization or as required by paragraph (a)(3)(ii)(B) of this section? (A)	
164.308(a)(4)(i)	Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(A)	If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect EPHI from the larger organization? (A)	
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? (A)	
164.308(a)(4)(ii)(C)	Have you implemented policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user's right of access to a workstation, transaction, program, or process? (A)	
164.308(a)(5)(i)	Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).	
164.308(a)(5)(ii)(A)	Do you provide periodic information security reminders? (A)	
164.308(a)(5)(ii)(B)	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	
164.308(a)(5)(ii)(C)	Do you have procedures for monitoring login attempts and reporting discrepancies? (A)	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords? (A)	
164.308(a)(6)(i)	Security Incident Procedures: Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or know security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes? (R)	
164.308(a)(7)(i)	Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.	
164.308(a)(7)(ii)(A)	Have you established and implemented procedures to create and maintain retrievable exact copies of	

	EPHI? (R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of EPHI data that is stored electronically? (R)	
164.308(a)(7)(ii)(C)	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode? (R)	
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans? (A)	
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? (A)	
164.308(a)(8)	Have you established a plan for periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart? (R)	
164.308(b)(1)	Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only of the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.	
164.308(b)(4)	Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances required by paragraph (b)(1) of this section that meets the applicable requirements of Sec. 164.314(a)? (R)	
	Physical Safeguards	
164.310(a)(1)	Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	
164.310(a)(2)(i)	Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency? (A)	
164.310(a)(2)(ii)	Have you implemented policies and procedures to safeguard the facility and the equipment therein	

	from unauthorized physical access, tampering, and theft? (A)	
164.310(a)(2)(iii)	Have you implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision? (A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks)? (A)	
164.310(b)	Have you implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI? (R)	
164.310(c)	Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users? (R)	
164.310(d)(1)	Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.	
164.310(d)(2)(i)	Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? (R)	
164.310(d)(2)(ii)	Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? (R)	
164.310(d)(2)(iii)	Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement? (A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of EPHI, when needed, before movement of equipment? (A)	
	Technical Safeguards	
164.312(a)(1)	Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining for obtaining necessary EPHI during and emergency? (R)	

164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt EPHI? (A)	
164.312(b)	Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI? (R)	
164.312(c)(1)	Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed? (R)	
164.312(e)(1)	Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of? (A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)	